ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
NOVEMBRE 2018

INFRASTRUTTURE CRITICHE: COSA SERVE PER PROTEGGERLE

LUISA FRANCHINA

AIIC

Nel mondo moderno le Infrastrutture Critiche (IC) costituiscono i gangli vitali della vita di ogni paese. Per questo motivo le IC in genere, e più in particolare quelle che operano nello spazio cibernetico, sono destinatarie di una serie di misure di tutela sia di tipo normativo che di tipo operativo.

La prova della costante tendenza finalizzata a creare e applicare una normativa per la protezione è data dalle iniziative europee intraprese per definire la "common strategy".

La recente Direttiva n. 2016/1148 ha definito, per tutti i Paesi dell'Unione, le misure atte a garantire un elevato livello comune di sicurezza delle reti e dei sistemi informativi: si tratta della cosiddetta direttiva NIS del 6 luglio 2016 che costituisce un elemento concreto all'interno della strategia europea di rafforzamento della sicurezza cibernetica.

La direttiva vuole promuovere il miglioramento dell'affidabilità e della sicurezza dei sistemi informativi il cui impiego costituisce, tra l'altro, un volano del mercato interno dell'UE.

In tema di promozione della sicurezza delle reti, oltre a prevedere misure operative comuni in materia di pianificazione, scambio di informazioni operative, resilienza e cooperazione, definisce gli obblighi comuni di sicurezza e introduce gli "operatori di servizi essenziali" e i "fornitori di servizi digitali" quali preposti all'adozione delle misure di sicurezza.

La Direttiva è entrata in vigore nell'agosto del 2016 e, muovendosi nel contesto dell'attuazione dei principi sanciti nella direttiva, l'Italia, la ha recepita nell'ordinamento giuridico nazionale con il D. Lgs. del 18 maggio 2018, n. 65, con il quale ha istituito le autorità nazionali competenti ed il Punto di Contatto Unico.

Il quadro europeo completo comprende anche il Regolamento Generale sulla Protezione dei Dati (GDPR) pubblicato sulla Gazzetta Ufficiale Europea il 4 maggio 2016.

D'altra parte, l'individuazione di standard e requisiti minimi, peraltro auspicata da anni e tuttora oggetto di dibattito,

Luisa Franchina, presidente AIIC (Associazione Italiana esperti in Infrastrutture Critiche)

non può costituire da sola la leva per promuovere la voluta concreta cultura della sicurezza.

L'ITU ha emanato una nuova linea guida[1] per la realizzazione di strategie nazionali di cyber security. Un capitolo è dedicato alla protezione delle IC e suggerisce, una volta identificati standard, adottati i meccanismi di gestione delle responsabilità e stabilita la politica di gestione del rischio, di identificare leve di mercato e promuovere la cooperazione pubblico privato.

La linea guida conferma che, a livello procedurale, è ormai riconosciuta internazionalmente l'importanza di:

- coinvolgere tutti i vari stakeholder nazionali all'interno di un contesto di cooperazione, dialogo e coordinamento, di fatto costituendo meccanismi chiari ed espliciti di condivisione dell'informazione (information sharing) a livello settoriale e intersettoriale;

- definire come gestire il rischio derivante dalla minaccia cibernetica e cosa si intenda per compliance necessaria alla sua riduzione;

- identificare e realizzare meccanismi di partnership tra pubblico e privato per far condividere a tutto il Sistema Paese il compito di proteggersi.

L'inadeguatezza dell'assetto normativo ad assecondare la veloce mutazione delle minacce avvalora il tema della scelta di leve di mercato. In particolare, un sistema basato sulla rilevanza della forma scritta a garanzia della certezza del diritto, entra in crisi nel serrato confronto con le tecnologie, che, per il loro intrinseco "being in progress", lo costringono ad un aggiornamento e conseguente adeguamento costanti.

Le risorse disponibili per creare una vera e propria struttura difensiva di livello così elevato sono esigue. La tutela delle IC mediante la prevenzione delle minacce, ad esempio attraverso il mantenimento dei sistemi aggiornati, necessita un flusso costante di risorse economiche.

Al riguardo, va considerato che uno Stato deve essere considerato come un "insieme unico" dal punto di vista della protezione: da un lato, infatti, la minaccia cyber si rivela ostile contro qualsiasi tipo di target, dall'altro la congruenza e la sistematicità degli interventi (siano essi a protezione di infrastrutture pubbliche o private, civili o militari, periferiche o centrali) garantiscono economie di scala, visione sistemica, cooperazione e condivisione delle informazioni sulle contromisure, equo livello di sicurezza in tutti i settori del Paese.

Rispetto alle "leve alternative" al supporto pubblico, si è anche ipotizzato[2] che un intervento dei privati potrebbe essere una scelta vincente.

L'apporto di capitali privati potrebbe sostenere il livello dei flussi finanziari da impiegare per proteggere le IC. Si apre il tema della nazionalità del finanziatore e soprattutto nel caso di grandi operazioni si immette la procedura della golden share: il tema della "nazionalizzazione" degli interventi va di pari passo con il tema della nazionalizzazione delle soluzioni. La sicurezza è fatta di hardware oltre che di software e parte dai dispositivi che usiamo, passando per le tecnologie di supporto fisico dell'ICT (information and communication technology). Ogni pezzo che costituisce la catena del valore attraverso la quale usufruiamo di un servizio coopera alla sicurezza del servizio stesso. Di conseguenza anche quando decidiamo di utilizzare una parte (una tecnologia, un dispositivo) della catena realizzato in altri Paesi dovremmo preoccuparci di "qualificarlo" o comunque di qualificare il produttore, secondo i termini attualmente in uso. La qualificazione è un processo che va standardizzato; in ogni caso la tendenza che sta emergendo è quella di caratterizzare l'esito della qualificazione secondo tre direttrici: competenza, rispondenza ai requisiti, indipendenza e neutralità. Una soluzione analoga potrebbe essere pensata per la verifica degli investitori e della loro "vision" nell'investimento.

1. ITU 2018 International Telecommunication Union (ITU) Guide to Developing a National Cybersecurity Strategy
2. Sulla tematica vedasi "Più capitali privati per rilanciare le infrastrutture" di Gianfranco Leonetti e Umberto Triulzi su il Sole 24ore del luglio 2018